Tracking and Updating Downstream Disclosures of Private Information

Response to RFI for National Privacy Research Strategy, 79 FR 56091 (September 18, 2014)

October 17, 2014

John M. Willis, President
pINFOSEC, Inc.
CISSP, ECSA, NSA-IEM, NSA-IAM
CEH, Security+, Linux+, CITRMS
CIPP/US, CIPP/G, CIPT
2020 Pennsylvania Ave NW #400
Washington DC 20006
John.Willis@pINFOSEC.com
LinkedIn.com/in/johnmwillis
(202) 670-7179

When managing the collection, retention, and dissemination of sensitive data the following Fair Information Practice Principles (FIPPs) are of particular interest:

> Transparency - Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
>
> Individual Participation - Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
>
> Use Limitation - Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
>
> Data Quality and Integrity - Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
>
> Accountability and Auditing - Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Today's solutions to these principles are generally satisfied at a high level. Consumers are notified that their information will be disclosed to various third parties as necessary for the purpose of providing a product or service, and sometimes to marketing and other organizations. Consumers have limited visibility into exactly who their private information is disclosed to. Organizations also have various challenges tracking specific disclosures.

When a consumer finds private information to be inaccurate that needs to be updated, they might be able to update it with the organization they have the relationship with, but the downstream consequences of the update are not well defined.

In a given consumer transaction there are various stakeholders of the data. The organization providing the product or service has its position as to who owns which data. The consumer has their own perspective as well. The organization's downstream liability for updates to specific data items may be unclear due to the ownership question.

When assessing whether or not an organization and its downstream partners are in compliance with various laws, it is challenging to track downstream disclosures of specific private data.

All of the above suggest that a more standardized approach to the issue of tracking and updating disclosures of private information is needed. A combination of architecture, process engineering, and legal expertise would be needed to provide direction. The end solution could be industry based in a manner similar to the National Strategy for Trusted Identities in Cyberspace (NSTIC), and perhaps further entrenched into legislation and regulations. Such a multidisciplinary effort would establish a framework that would clarify stakeholder liability positions and provide transparency to the consumer.

For examples of how technology has been applied to handle such disclosures the manner in which law enforcement tracks certain private information is a key example. There are certainly other examples in the health care field, as well as with passport information, that would be instructive. All of these examples have certain elements in common that should be taken into consideration in standardizing a consumer private data infrastructure.

Some specific examples of implementations and research include:

> Cascading Disclosure-Control Language (CDCL) is a simple, transparent, high-confidence mechanism for declaring rules of disclosure. It is a language and framework built expressly for item-level disclosure control. The CDCL was created by the State of Wisconsin, Office of Justice Assistance, Wisconsin Justice Information Sharing (WIJIS) Program.
>
> The Information Exchange Package Documentation (IEPD) Clearinghouse provides information on a variety of IEPDs that have been submitted by individuals and organizations who have implemented the Global Justice XML Data Model (GJXDM) and the National Information Exchange Model (NIEM).

The primary barrier to defining and implementing a standard for collection, tracking and updating downstream disclosures of private data is that organizations have their own interests, which are, to an extent, at odds with the consumer. However, as with any standardization effort the biggest challenge is realizing the need and convening all of the stakeholders.